UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/761,373	01/16/2001	Paul Cador Roberts	13768.191	5334

22913 7590 08/23/2004

WORKMAN NYDEGGER (F/K/A WORKMAN NYDEGGER & SEELEY)
60 EAST SOUTH TEMPLE
1000 EAGLE GATE TOWER
SALT LAKE CITY, UT 84111

EXAMINER	
TRAN, TONGOC	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 08/23/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/761,373	ROBERTS, PAUL CADOR	
	Examiner	Art Unit	
	Tongoc Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 January 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *1/16/2001*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to applicant's application serial no. 09/761,373 filed on 1/16/2001.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 1/16/2004 has been considered by the examiner.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-2, 4, 7-8, 10-17, 21-23, 25, 28-29 and 31-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jones (U.S. Patent No. 5,412,730) in view of Thompson et al. (U.S. Patent No. 6,357,046, hereinafter Thompson).

In respect to claim 1, Jones discloses in a network system that includes a first computer system network connectable to a second computer system, the first computer system capable of encrypting data, a method of the first computer system encrypting data so as to guard against eavesdropping and brute force attacks, the method comprising the following (Jones, Abstract):

an act of securely negotiating a master secret with the second computer system (Jones, col. 9, line 50-col. 10, line 20);

an act of generating a random bit sequence (Jones, col. 1, lines 37-53);

an act of including the random bit sequence in a seed to generate a random seed (Jones, col. 1, lines 37-53);

an act of inputting the master secret and the random seed into a key generation module to generate a key; an act of using the key to encrypt data (Jones, col. 1, lines 37-col. 2, line 50); and

Jones does not disclose but Thompson discloses an act of including the encrypted data and the random seed in a data structure (Thompson, col. 3, lines 27-44 and col. 7, line 25-57). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate Thompson's teaching of including the encrypted data with the random seed in a data structure with Jones' teaching of randomly altering encryption key so that new key can be calculated synchronously at both sender and receiver to accommodate the frequent changed of random seed keys.

In respect to claim 2, Jones and Thompson disclose the method in accordance with Claim 1, wherein the data structure is a data packet, the method further comprising an act of transmitting the data packet in accordance with a protocol (Thompson, col. 3, lines col. 3, lines 27-44).

In respect to claim 4, the claim limitation is substantially similar to claim 1. Therefore, claim 4 is rejected based on the similar rationale.

In respect to claim 7, Jones and Thompson disclose the method in accordance with Claim 1, further comprising an act of negotiating a parameter expiry with the second computer system, the parameter expiry indicating the lifetime of the master secret (Jones, col. 9, lines 50-68).

In respect to claim 8, Jones and Thompson disclose the method in accordance to Claim 7, wherein upon expiration of the lifetime of the master secret, performing an act securely renegotiating a master secret with the second computer system (Jones, col. 9, lines 50-68).

In respect to claim 10, Jones and Thompson disclose the method in accordance with Claim 1, wherein the act of generating a random bit sequence is performed by a cryptographically secure random number generator (Jones, Abstract).

In respect to claim 11, Jones and Thompson disclose the method in accordance with Claim 1, further comprising an act of including, in the random seed, a bit sequence that represents the current time (Jones, col. 3, lines 56-col. 4, line 12).

In respect to claim 12, Jones and Thompson disclose the method in accordance with Claim 1. Jones and Thompson do not explicitly disclose wherein the random seed is at least 96 bits. However, it is well known that the longer the key, the more difficult it is to break. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to provide a random seed of at least 96 bits for more secure keys.

In respect to claims 13, 15, 22-23, 25, 33 and 35, the claim limitations are substantially similar to claim 1. Therefore, claims 13, 15, 22-23, 25, 33 and 35 are rejected based on the similar rationale.

In respect to claims 16-17, 28-29, 21 and 31-32, the claim limitations are substantially similar to claims 2, 4, 7-8 and 11-12. Therefore, claims 16-17, 28-29, 21 and 31-32 are rejected based on the similar rationale.

In respect to claims 14 and 34, Jones and Thompson disclose the computer program product as recited in claim 13 and 33, wherein the computer-readable medium is a physical storage medium (Jones, Abstract).

4. Claims 3, 5-6, 9, 18-20, 24, 26-27, and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jones (U.S. Patent No. 5,412,730) in view of Thompson et al. (U.S. Patent No. 6,357,046, hereinafter Thompson) and further in view of Patel (U.S. Patent No. 6,327,660).

In respect to claim 3, Jones and Thompson disclose the method in accordance with. Claim 2. Both Jones and Thompson do not disclose but Patel discloses the data packet includes a security Parameter Index in accordance with the Encapsulating Security Payload (ESP) (Patel, col. 4, line 27-col. 5, line 5). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teaching of Jones and Thompson's teaching of randomly altering encryption key in an encrypted data transmission with Patel's teaching of including a security parameter

index in accordance with encapsulating security payload in the data packet to protect the integrity and confidentiality of information transmitted over network.

In respect to claims 5-6 and 9, Jones and Thompson disclose the method in accordance with Claims 1 and 2. Jones and Thompson do not explicitly disclose but Patel discloses a wireless communication and an protocol comprises an unconfirmed push protocol wherein the unconfirmed push protocol comprises User Datagram Protocol (UDP) (Patel, col. 2, lines 48-67, UDP and unconfirmed push protocol is inherent in wireless communication). It would have obvious to one of ordinary skill in the art at the time the invention was made to incorporate Patel's wireless communication protocol with Jones and Thompson's encrypted data transmission over a communication network for the benefit of mobility.

In respect to claims 18-20, 24, 26-27 and 30, the claim limitations are substantially similar to claims 3, 5-6 and 9. Therefore, claims 18-20, 24, 26-27 and 30 are rejected based on the similar rationale.

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Rubinstein et al. Disclose system and method of dynamic key generation for digital communication.

-Schneier, B. "Applied Cryptography, Protocols, Algorithms, and Source Code in C, Second Edition", pages 169-187.

Gammie et al. Disclose method and apparatus for uniquely encrypting a plurality of services at a transmission site.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tongoc Tran whose telephone number is (703) 305-7690. The examiner can normally be reached on 8:30-5:00 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Examiner: Tongoc Tran
Art Unit: 2134

TT

August 16, 2004

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100